Dark Caracal - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:25:04 UTC

Description(Lookout) Lookout and Electronic Frontier Foundation (EFF) have discovered Dark Caracal, a persistent and prolific actor, who at the time of writing is believed to be administered out of a building belonging to the Lebanese General Security Directorate in Beirut. At present, we have knowledge of hundreds of gigabytes of exfiltrated data, in 21+ countries, across thousands of victims. Stolen data includes enterprise intellectual property and personally identifiable information. We are releasing more than 90 indicators of compromise (IOC) associated with Dark Caracal including 11 different Android malware IOCs; 26 desktop malware IOCs across Windows, Mac, and Linux; and 60 domain/IP based IOCs.

Dark Caracal targets include individuals and entities that a nation state might typically attack, including governments, military targets, utilities, financial institutions, manufacturing companies, and defense contractors. We specifically uncovered data associated with military personnel, enterprises, medical professionals, activists, journalists, lawyers, and educational institutions during this investigation. Types of data include documents, call records, audio recordings, secure messaging client content, contact information, text messages, photos, and account data.

ObservedSectors: Defense, Education, Financial, Government, Healthcare, Manufacturing, Media, Utilities and activists, lawyers and journalists.
Countries: China, France, Germany, India, Italy, Jordan, Lebanon, Nepal, Netherlands, Pakistan, Philippines, Qatar, Russia, Saudi Arabia, South Korea, Switzerland, Syria, Thailand, USA, Venezuela, Vietnam.
